12 Jul 22

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

Vulnerable IP Devices Exposed via MITRE Security Advisory

A security advisory for a vulnerability by MITRE has inadvertently exposed links to remote admin consoles. The incident came to light after a reader tipped off BleepingComputer about links to exposed systems listed within the references section. The reference links lead the readers to a remote administration dashboard of the exposed IP cameras or video devices, allowing any users to watch live camera feed or exploit the flaw.

https://cyware.com/news/vulnerable-ip-devices-exposed-via-mitre-security-advisory-10dd9fb5/?&web_view=true

Hackers Used Fake Job Offer on LinkedIn to Target Axie Infinity

It has emerged that the $540-million hack of Axie Infinity's Ronin Bridge in March 2022 was the consequence of one of its former employees getting tricked by a fraudulent job offer on LinkedIn. Allegedly, a senior engineer at the company was tricked into applying for a job at a nonexistent company, prompting the individual to download a fake offer document disguised as a PDF. The offer document acted as a vessel to deploy malware designed to breach Ronin's network, leading to one of the crypto sector's largest hacks to date.

https://www.itsecurityguru.org/2022/07/11/hackers-used-fake-job-offer-on-linkedin-to-target-axie-infinity/?utm_source=rss&utm_medium=rss&utm_campaign=hackers-used-fake-job-offer-on-linkedin-to-target-axie-infinity

Anubis Networks is Back With New C2 Server

Anubis Network is a command and control (C2) portal developed to control fake portals and aims to steal credentials to fully access the real systems. A large-scale phishing campaign has been targeting Internet end users in Brazil and Portugal since March 2022. The Anubis network phishing campaigns are masked through the CloudFlare CDN. Operators can easily make this configuration through an interface that uses the CloudFlare API for configuring new DNS zones.

https://securityaffairs.co/wordpress/133115/hacking/anubis-networks-new-c2.htm

Fake Google Software Updates Spread New Ransomware

Threat actors are increasingly using fake Microsoft and Google software updates to try to sneak malware onto target systems. Researchers from Trend Micro recently discovered this in the wild disguised as a Google Software Update application. "HavanaCrypt" is .Net malware that uses an open-source tool called "Obfuscar" to obfuscate its code. Once deployed on a system, HavanaCrypt first checks to see if the "GoogleUpdate" registry is present on the system, and only continues with its routine if the malware determines the registry is not present.

https://www.darkreading.com/attacks-breaches/attacker-using-fake-google-software-update-to-distribute-new-ransomware

CEO Accused of Making Millions via Sale of Fake Cisco Devices

The U.S. Department of Justice announced on Friday that a man has been arrested and charged for allegedly selling fraudulent and counterfeit Cisco products. The fake products had counterfeit Cisco labels, stickers, boxes, and documentation to appear new, genuine, and of high quality.

https://www.securityweek.com/ceo-accused-making-millions-sale-fake-cisco-devices